Raytheon
BBN Technologies

BBN Technologies
10 Moulton Street
Cambridge, MA 02138

30 October 2014

Office of Naval Research
875 North Randolph Street, Suite 1179
Arlington, VA 22203-1995

Delivered via Email to:
carey.schwartz@navy.mil
reports@library.nrl.navy.mil
tr@dtic.mil
shannon.viverette@navy.mil

Contract Number:	N00014-14-C-0002
Proposal Number:	P13003-BBN
Contractor Name and PI:	Raytheon BBN Technologies; Dr. Jonathan Habif
Contractor Address:	10 Moulton Street, Cambridge, MA 02138
Title of the Project:	Seaworthy Quantum Key Distribution Design and Validation (SEAKEY)
Contract Period of Performance:	7 February 2014 – 7 February 2016
Total Contract Amount:	$475,359 (Base)
Amount of Incremental Funds:	$205,668
Total Amount Expended (thru 17 October):	$163,155

Attention: Dr. Carey Schwartz
Subject: Quarterly Progress Report
Reference: Exhibit A, CDRLs

In accordance with the reference requirement of the subject contract, Raytheon BBN Technologies (BBN) hereby submits its Quarterly Progress Report. This cover sheet and enclosure have been distributed in accordance with the contract requirements.

Please do not hesitate to contact Dr. Habif at 617.873.5890 (email: jhabif@bbn.com) should you wish to discuss any technical matter related to this report, or contact the undersigned, Ms. Kathryn Carson at 617.873.8144 (email: kcarson@bbn.com) if you would like to discuss this letter or have any other questions.

Sincerely,
Raytheon BBN Technologies

Kathryn Carson

Kathryn Carson
Program Manager
Quantum Information Processing

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **30 OCT 2014**	2. REPORT TYPE	3. DATES COVERED **00-00-2014 to 00-00-2014**

4. TITLE AND SUBTITLE **Seaworthy Quantum Key Distribution Design and Validation (SEAKEY)**	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **BBN Technologies,,10 Moulton Street,,Cambridge,,MA,02138**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S) 11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

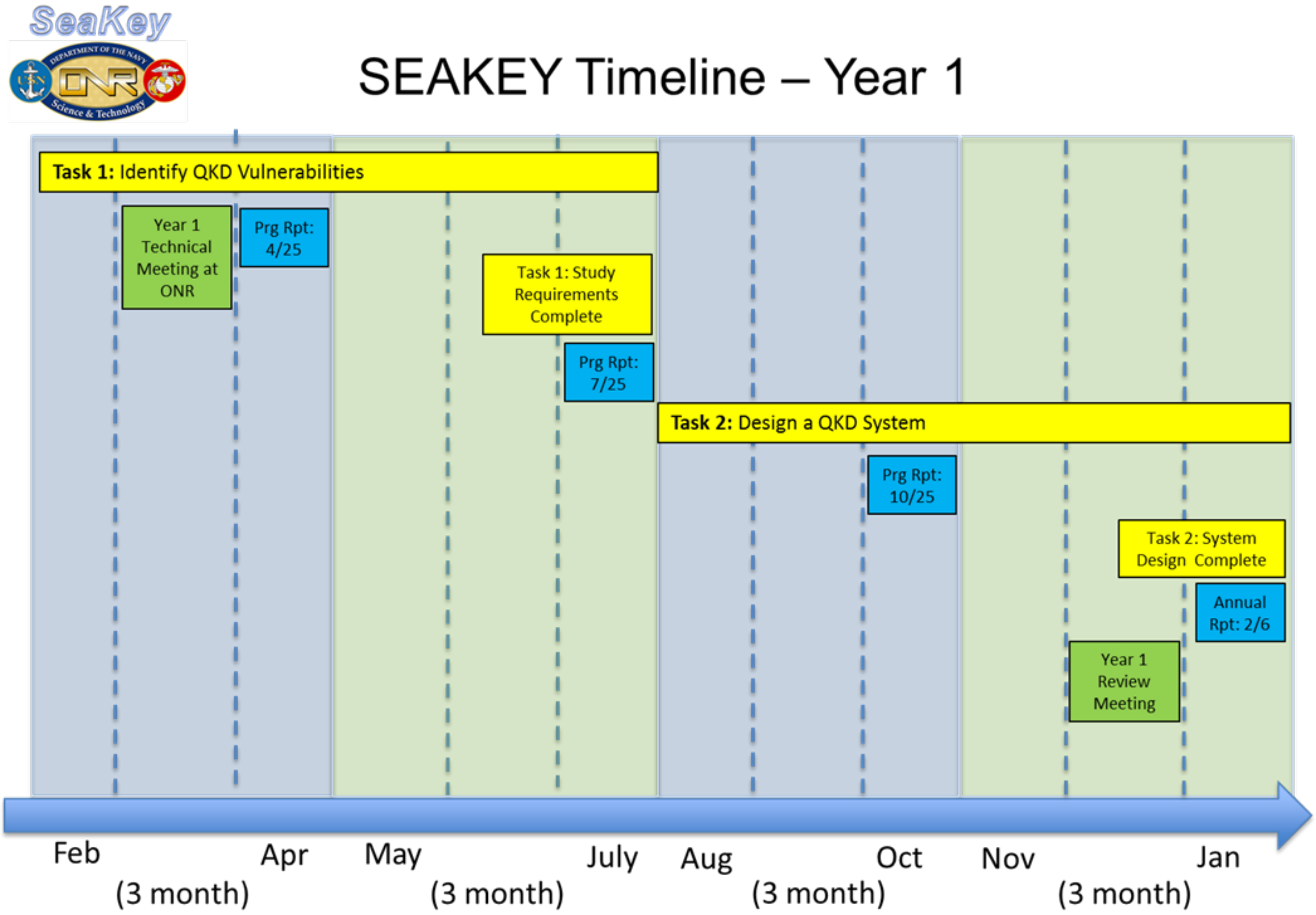
15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**9**	

SEAKEY Quarterly Progress Report for the Period 26 July 2014 – 24 October 2014

Section A. Project Schedule

The Year 1 timeline below identifies SeaKey tasks, their duration, task milestones, kickoff meeting, tentative program review meeting, and progress report due dates.



Section B. Technical Progress

In this report we summarize the technical progress accomplished during the third quarter of work of the SeaKey program.

Key-rate versus loss, and comparison of protocols

Figure 1 shows the secret key rate vs. end-to-end channel loss, for various QKD protocols, without the use of quantum repeaters. The key points to note are,

(i) CV and DV protocols have same optimal rate-loss scaling, R~η,

(ii) CV binary-phase-shift-keying (BPSK) and DV (polarization, or time-bin encoded) BB84 without decoy states, both yield a worse (R~η^2) scaling, and

(iii) We believe that an extension of the CV BPSK protocol with a few additional modulation levels (but far fewer from a QAM-sampled discretization of the full Gaussian distribution of amplitude and phase, that CV demonstrations use) should retrieve the optimal (R~η) key rate scaling. This would be same effect that decoy yields for DV. The security analysis of this is currently being done.

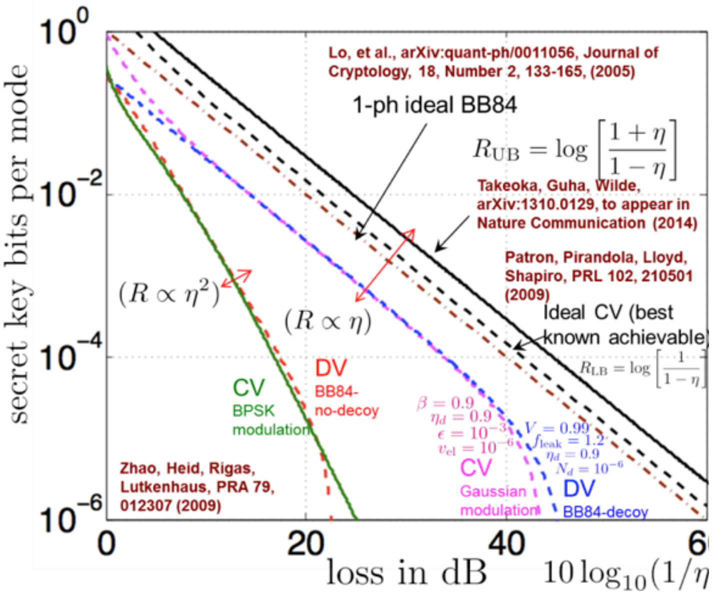


Fig. 1. Rate vs. loss

While the fundamental rate trade-offs show similar trends for CV and DV, CV protocols have lower noise (being only limited by local-oscillator shot-noise of the coherent-detection receiver) and can access a higher number of modes/second, because homodyne or heterodyne detection can potentially have a much higher bandwidth compared to single photon detection, at comparable detection efficiencies. On the other hand, error-correction codes are better developed for small-alphabet DV protocols. Because DV protocols have small discrete signaling constellations, modulation is simpler, as compared to CV protocols (where symbols must be chosen from a Gaussian distribution or a densely-quantized version thereof). This increases the local randomness requirement for CV implementations more severe.

Ongoing work: Our extension of the CV-BPSK protocol that only uses a few modulation constellation points, while achieving the R~η rate-loss scaling, we believe will ease on the aforesaid hardest obstacle to CV implementations, while preserving the benefits of faster detectors.

Direct-secure communication with laser light

We have invented a direct communication protocol, that is quantum secure to a passive eavesdropper (same benchmark of security as the Shapiro two-way protocol), but requires only a simple one-way binary-phase laser-light signaling, near-LO-shot-noise-limited homodyne detection, and a reverse authenticated public classical channel (which may be an RF link for instance). The bits/mode performance of this protocol is several orders of magnitude better than the Shapiro protocol, which needs entangled states. The bits/mode performance achieved by our protocol adheres the quantum-limited rate-loss scaling (R~η), and is only factor of 2 to 3 below it for reasonable assumptions on sources and homodyne detection. The Shapiro protocol enjoys a big modes/sec number due to the inherently broadband SPDC sources, resulting in a good bits/sec performance (despite the poor bits/mode performance).

Ongoing work: (1) We are currently investigating an extension of our laser-light direct-secure communication protocol, which still uses a BPSK modulation, but uses a collection of spreading sequence to code-division multiplex the transmit signal, and uses a broadband homodyne detection. This frequency spreading will tremendously enhance the modes/sec available, and with our already excellent bits/mode performance, will yield a very high rate direct secure link for 10-30 km range. (2) We are also concurrently looking into extending this analysis to incorporate the "covertness" aspect (LPD), on top of the security (LPI) aspect.

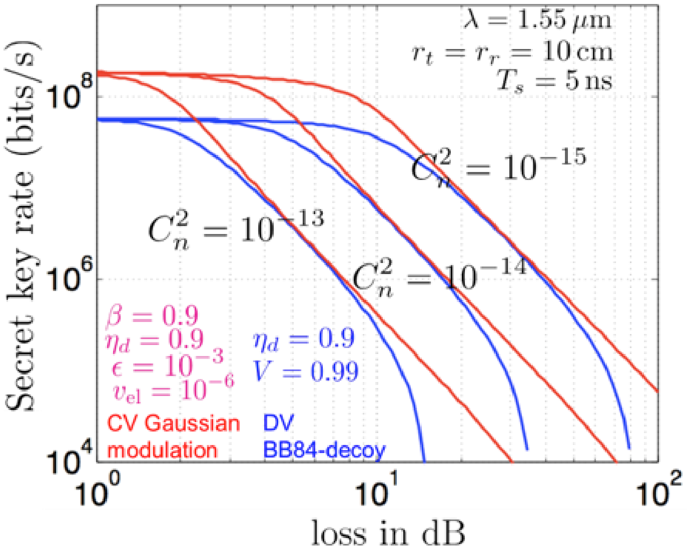


Fig. 2. Effect of turbulence strength

QKD in the presence of turbulence

The performance of CV Gaussian and DV BB84 protocols with variation in atmospheric turbulence is shown in Figure 2, which plots the secret key rates as a function of channel loss. We assume the fundamental Gaussian beam is modulated, and assume circular apertures. For this plot, all the "loss" has been lumped into one dB figure (the x axis), which could have contributions from diffraction-limited beam-spread, atmospheric scattering due to aerosols and water vapor, and any coupling efficiency loss at the receiver—for instance the free-space to fiber mode coupling efficiency in a fiber-coupled detector. Realistic device parameters (as listed in the plot legend) were chosen for both CV and DV implementations. As expected, the key rate vs. loss degrades with increasing C_n^2. Roughly speaking, one order of magnitude increase in C_n^2 results in the key rates to diminish by one order of magnitude.

Ongoing work: We are working on incorporating turbulence strength variation through propagation and also turbulence-strength variation as a function of elevation from the sea floor. The MODTRAN database, which we used for generating the results in #d below, does not incorporate turbulence. Our partners at Raytheon Vision Systems have acquired a software for numerical turbulence modeling through the atmosphere, which we are currently incorporating.

QKD with all atmospheric detriments: a wavelength comparison

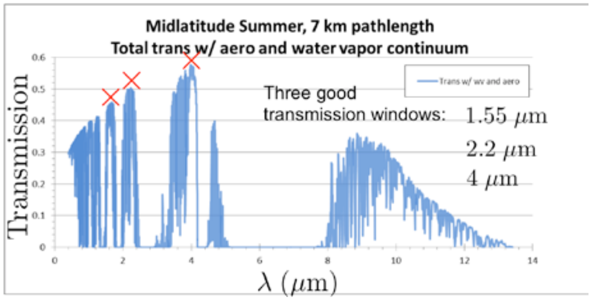


Fig. 3. Atmospheric transmission

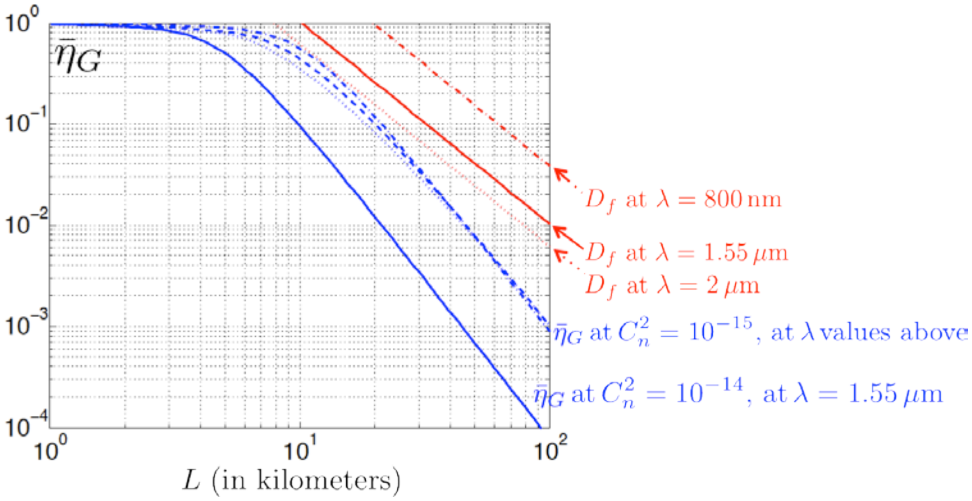
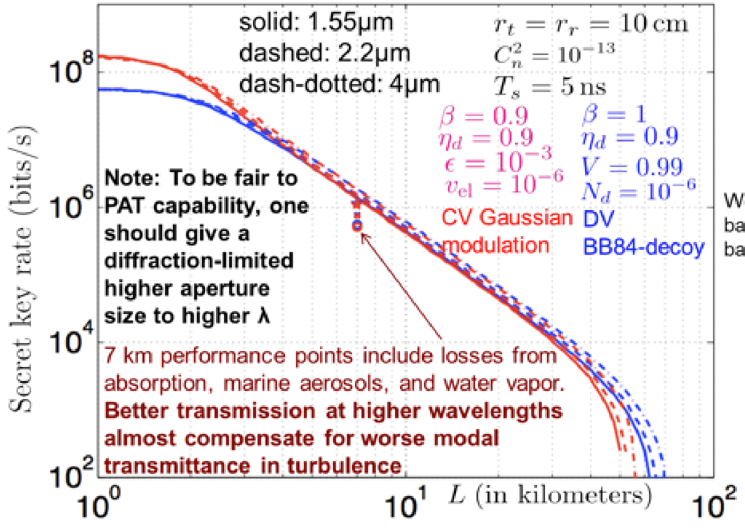


Fig. 4. Turbulent propagation with varying wavelength

The evaluation of BB84 key-rate vs. loss performance in the presence of standard marine non-idealities, was carried out utilizing parameter inputs generated by the MODTRAN database, and compared for three wavelengths (see Fig. 3). The wavelengths chosen (1550nm, 2.2 μm, 4μm) were based on finding a "sweet spot" in the trade-space of good atmospheric transmission (see Fig. 3 for a representative sample plot generated via MODTRAN), and a good background (combination of sky irradiance and blackbody). Interestingly, up to a certain distance (roughly upto 30 km—the SeaKey relevant range), the higher wavelengths have worse transmission, whereas beyond that range, the order reverses (see the blue plots at $C_n^2=10^{-15}$ in Fig. 4). In Fig. 5, we plot the ensemble-average end-to-end diffraction-limited transmittance of the fundamental Gaussian mode, in the presence of turbulence. The better aerosol/water-vapor atmospheric transmission numbers at higher wavelengths almost fully compensated for the worse mean diffraction-limited turbulent-channel modal transmittance at higher wavelength (that we saw above in the 0-30 km range), yielding very similar key rate performance across all three wavelengths we evaluated (see Fig. 5). Although the plot in Fig. 5 only includes these factors into a rate calculation only for one range (7 km), it clearly shows that the aforesaid opposing effects make the wavelength choice really upon the ease of transmitter-modulation and receiver-detection (CV/DV-considered) availability. As one final point, note in Fig. 4, that going from 2 micron to 800 nm transmission, the free-space Fresnel number product D_f, a rough estimate of the number of orthogonal spatial modes that can be simultaneously transmitted increases by an order of magnitude, which is a factor that favors transmitting on shorter wavelengths, all else remaining equal.



We considered 3 wavelengths, based on transmission background tradeoff

Fig. 5. QKD over atmospheric channel: wavelength comparison

Ongoing work: We are currently putting together a software tool implemented in MATLAB, which talks to the MODTRAN database via an intermediate numerical dump of transmission data across a wide range of parameters, which will enable us to tweak the various operating conditions and see the sensitivity of the QKD system's rate performance with various parameters such as visibility, operating condition for aerosols (maritime, mid-latitude summer, etc.), elevation, wavelength, background level, etc. In the current version of the tool, the user can set the following choices:

(1) Atmospheric model (MLS/US76/Tropical)

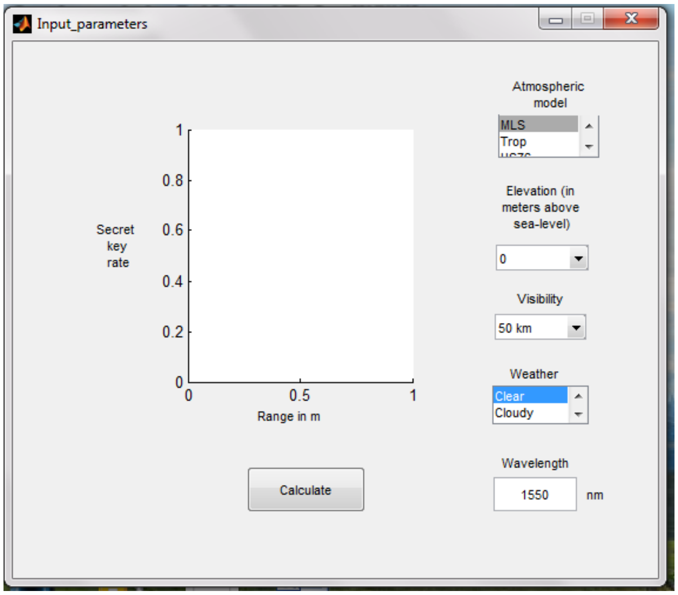
(2) Elevation above sea-level in m (0/10/20)

(3) Aerosol concentration (corresponding to visibility of 50km/23km/5km)

(4) Weather conditions (clear/cloudy/hazy/rainy)

(5) Wavelength of operation (can be user-defined between 1.49μm and 4.17μm)

Fig.5 shows the current form of the GUI.



Elevation (in meters above sea-level): 0

Visibility: 50 km

Wavelength: 1550 nm

Fig. 5. GUI which plots secret key rate of the BB84 and CV protocols in the presence of user-specified nonidealities.

The current version of the program uses default values of background count rates (10^{-6}/pulse for DV, and 0.001 photons/mode optical noise for CV). In the next couple of weeks, the program will be modified to include background count rates calculated from sky radiance and blackbody radiance, which is obtained from user-defined values of solar elevation angle and weather conditions.

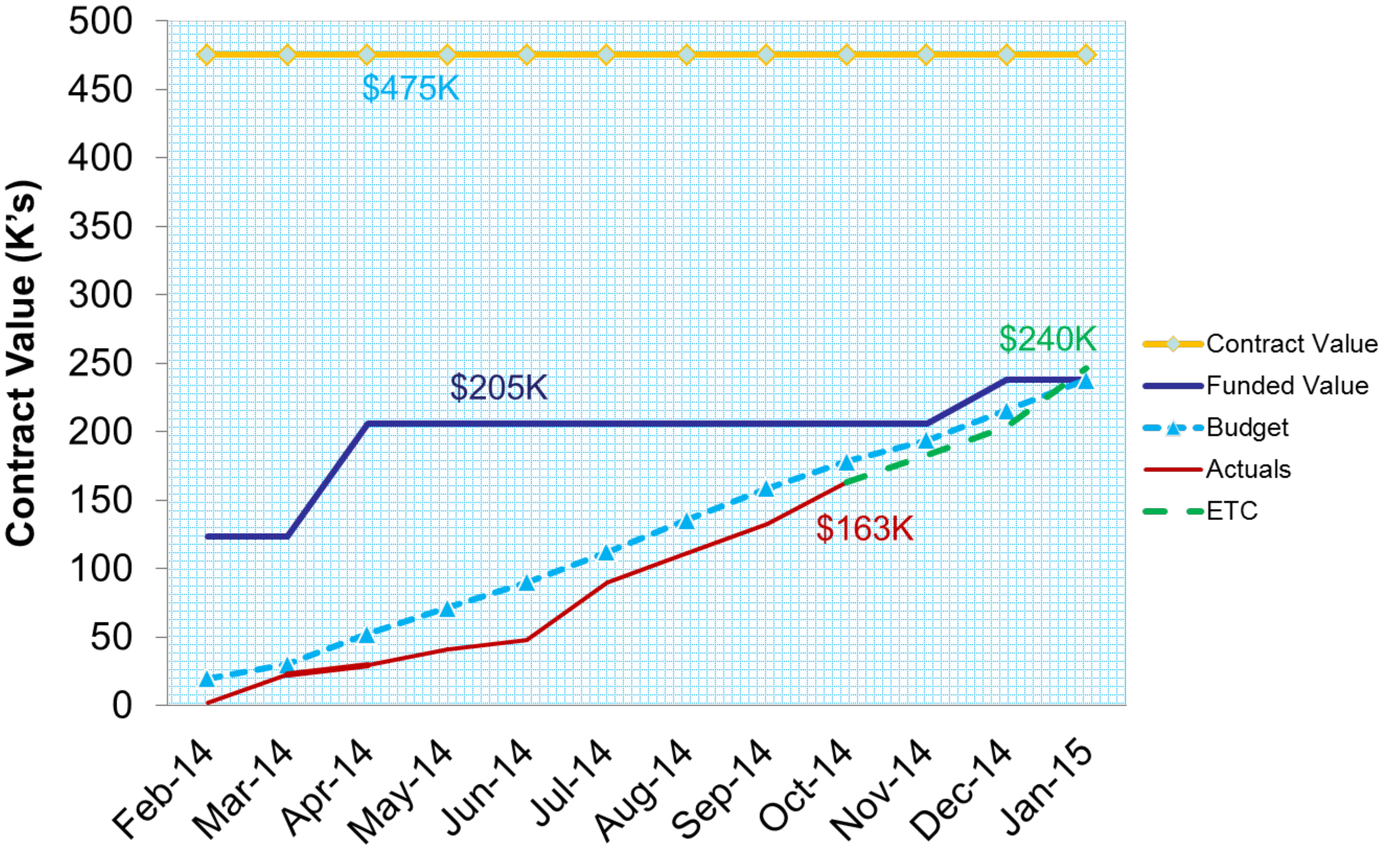
This software tool will also enable reverse engineer requirements on sources and detectors required so as to for instance make 2.2 μm an attractive wavelength for naval QKD. This tool will also generate the value of the Fresnel number product D$_f$, and will have the ability to “turn on” multi-spatial-mode operation, and choose up to a certain number of spatial modes with mode spacing specified as input (the software will calculate spatial mode cross talk and incorporate that into the rate calculations). Finally, this tool will not just be limited to QKD, but will be easily ported to calculate the rates for direct secure communication protocols, and other quantum communication protocols for instance.

C. Problem Areas – Identification

There are no anticipated problems or issues to report at this time.

Section D. SEAKEY Financial Update

Financial Chart reflecting Year 1:


Contract Value (K's)
$475K
$205K
$240K
$163K
Feb-14
Mar-14
Apr-14
May-14
Jun-14
Jul-14
Aug-14
Sep-14
Oct-14
Nov-14
Dec-14
Jan-15
Contract Value
Funded Value
Budget
Actuals
ETC